Amendments to the Claims

Claim 1 (currently amended): In a computing environment having a plurality of secure network connections ~~connection to a network~~, a computer program product for securely propagating security credentials using a trusted master registry, the computer program product embodied on one or more computer-readable media and comprising:

~~computer-readable program code means for establishing a secure connection between a client and a password synchronization agent (PSA);~~

computer-readable program code means for receiving, ~~at the PSA~~ by a password synchronization agent ("PSA") from a user at a [[the]] client device over [[the]] a first secure connection between the client device and the PSA on which the PSA has authenticated itself to the client device, a password propagation request providing an identifier of [[a]] the user and an identifying secret of the ~~user during propagation request processing~~;

computer-readable program code means for ~~validating the user with the~~ forwarding, by the PSA to a trusted master registry over a second secure connection therebetween on which the trusted master registry has authenticated itself to the PSA, [[using]] the received user identifier and identifying secret, ~~on request of the PSA~~ wherein the trusted master registry stores identifying secrets for user identifiers only as secured, non-recoverable versions thereof;

computer-readable program code means for receiving, by the PSA from the trusted master registry over the second connection, a validation result created by the trusted master registry responsive to the forwarding, the validation result being a successful result if it indicates that the trusted master registry had previously stored, for the user identifier, a secured version of the identifying secret; and

computer-readable program code means for propagating, if the validation result is the successful result, the received user identifier and identifying secret ~~of the user directly~~ from the PSA to one or more target registries ~~if the validation succeeds~~ over third mutually-authenticated secure connections, each of the third connections being between the PSA and a distinct one of the target registries, such that each target registry can store, for the user identifier, a secured version of the identifying secret, wherein the secured version stored by the target registries is not required to be identical to the secured version stored at the trusted master registry.

Claims 2 - 3 (canceled)

Claim 4 (currently amended): The computer program product according to Claim 1, wherein the trusted master registry stores password synchronization policy information, and wherein the computer-readable program code means for propagating ~~the received identifying secret~~ further comprises computer-readable program code means for identifying the target registries using the stored password synchronization policy information for the user identifier.

Claim 5 (currently amended): The computer program product according to Claim 1, wherein the trusted master registry stores password synchronization policy information, and wherein the computer-readable program code means for propagating ~~the received identifying secret~~ further comprises computer-readable program code means for identifying the target registries using the stored password synchronization policy information for a user group of which the user identified by the user identifier is a member.

Claims 6 - 8 (canceled)

Claim 9 (currently amended): The computer program product according to Claim 1, wherein the previously-stored secured version of the identifying secret was created, at the trusted master registry, by ~~computer-readable program code means for validating further comprises:~~ ~~computer-readable program code means for~~ performing a security function on a previously-received copy of the ~~received~~ identifying secret of the user, wherein the security function comprises one of (i) a one-way hashing algorithm or (ii) an encryption algorithm; ~~computer-readable program code means for using the received user identifier to locate a previously-stored identifying secret of the user which was stored by the master registry, and~~ wherein the security function is repeated, at the trusted master registry, on the forwarded identifying secret of the user, after which, if a result thereof is identical to the previously-stored secured version, the trusted master registry then creates the successful result ~~computer-readable program code means for concluding that the validation succeeds if the located identifying secret is identical to a result of performing the security function.~~

Claim 10 (currently amended): The computer program product according to Claim 1, wherein the validation result is created, at the trusted master registry, by ~~computer-readable program code means for validating further comprises computer-readable program code means for~~ invoking an authenticated LDAP bind or other native authentication mechanism of the trusted master registry, using ~~wherein~~ the ~~received~~ forwarded user identifier ~~of the user and the received~~ identifying

secret of the user, and wherein the validation result is created using a result of the LDAP bind or other native authentication mechanism ~~are passed to the master registry, thereby causing the master registry to validate the passed identifier and identifying secret and return a result which reports a success or failure of the validation.~~

Claim 11 (original): The computer program product according to Claim 1, wherein the PSA has administrative authority for performing operations at the one or more target registries.

Claim 12 (currently amended): The computer program product according to Claim 1, further comprising:

computer-readable program code means for obtaining a new value from the user to be used as the propagated identifying secret if the validation ~~succeeds~~ result is the successful result; and

computer-readable program code means for substituting this new value for the received identifying secret prior to operation of the computer-readable program code means for propagating.

Claim 13 (currently amended): A system for securely synchronizing security credentials using a trusted master registry, comprising:

~~means for establishing a secure connection between a client and a password synchronization agent (PSA);~~

means for receiving, ~~at the PSA~~ by a password synchronization agent ("PSA") from a

user at a [[the]] client device over [[the]] a first secure connection between the client device and the PSA on which the PSA has authenticated itself to the client device, a password propagation request providing an identifier of [[a]] the user and an identifying secret of the user ~~during propagation request processing~~;

means for ~~validating the user with the~~ forwarding, by the PSA to a trusted master registry over a second secure connection therebetween on which the trusted master registry has authenticated itself to the PSA, [[using]] the received user identifier and identifying secret, ~~on request of the PSA~~ wherein the trusted master registry stores identifying secrets for user identifiers only as secured, non-recoverable versions thereof;

means for receiving, by the PSA from the trusted master registry over the second connection, a validation result created by the trusted master registry responsive to the forwarding, the validation result being a successful result if it indicates that the trusted master registry had previously stored, for the user identifier, a secured version of the identifying secret; and

means for propagating, if the validation result is the successful result, the received user identifier and identifying secret ~~of the user directly~~ from the PSA to one or more target registries ~~if the validation succeeds~~ over third mutually-authenticated secure connections, each of the third connections being between the PSA and a distinct one of the target registries, such that each target registry can store, for the user identifier, a secured version of the identifying secret, wherein the secured version stored by the target registries is not required to be identical to the secured version stored at the trusted master registry.

Claims 14 - 15 (canceled)

Claim 16 (currently amended): The system according to Claim 13, wherein the trusted master registry stores password synchronization policy information, and wherein the means for propagating ~~the received identifying secret~~ further comprises means for identifying the target registries using the stored password synchronization policy information for the user identifier.

Claim 17 (currently amended): The system according to Claim 13, wherein the trusted master registry stores password synchronization policy information, and wherein the means for propagating ~~the received identifying secret~~ further comprises means for identifying the target registries using the stored password synchronization policy information for a user group of which the user identified by the user identifier is a member.

Claims 18 - 20 (canceled)

Claim 21 (currently amended): The system according to Claim 13, wherein the previously-stored secured version of the identifying secret was created, at the trusted master registry, by ~~means for validating further comprises:~~

~~means for~~ performing a security function on a previously-received copy of the ~~received~~ identifying secret of the user, wherein the security function comprises one of (i) a one-way hashing algorithm or (ii) an encryption algorithm;

~~means for using the received user identifier to locate a previously-stored identifying secret of the user which was stored by the master registry; and~~

wherein the security function is repeated, at the trusted master registry, on the forwarded identifying secret of the user, after which, if a result thereof is identical to the previously-stored secured version, the trusted master registry then creates the successful result ~~means for concluding that the validation succeeds if the located identifying secret is identical to a result of performing the security function~~.

Claim 22 (currently amended): The system according to Claim 13, wherein the validation result is created, at the trusted master registry, by ~~means for validating further comprises means for~~ invoking an authenticated LDAP bind or other native authentication mechanism of the trusted master registry, using the forwarded user ~~wherein the received~~ identifier ~~of the user and the received~~ identifying secret of the user, and wherein the validation result is created using a result of the LDAP bind or other native authentication mechanism ~~are passed to the master registry, thereby causing the master registry to validate the passed identifier and identifying secret and return a result which reports a success or failure of the validation~~.

Claim 23 (original): The system according to Claim 13, wherein the PSA has administrative authority for performing operations at the one or more target registries.

Claim 24 (currently amended): The system according to Claim 13, further comprising:

means for obtaining a new value from the user to be used as the propagated identifying secret if the validation ~~succeeds~~ result is the successful result; and

means for substituting this new value for the received identifying secret prior to operation

of the means for propagating.

Claim 25 (currently amended): A computer-implemented method for securely propagating security credentials using a trusted master registry, comprising steps of:

~~establishing a secure connection between a client and a password synchronization agent (PSA);~~

receiving, by a password synchronization agent ("PSA") ~~at the PSA~~ from a user at a [[the]] client device over [[the]] a first secure connection between the client device and the PSA on which the PSA has authenticated itself to the client device, a password propagation request providing an identifier of [[a]] the user and an identifying secret of the user ~~during propagation request processing~~;

forwarding, by the PSA to a ~~validating the user with the~~ trusted master registry over a second secure connection therebetween on which the trusted master registry has authenticated itself to the PSA, [[using]] the received user identifier and identifying secret, ~~on request of the PSA~~ wherein the trusted master registry stores identifying secrets for user identifiers only as secure, non-recoverable versions thereof;

receiving, by the PSA from the trusted master registry over the second connection, a validation result created by the trusted master registry responsive to the forwarding, the validation result being a successful result if it indicates that the trusted master registry had previously stored, for the user identifier, a secured version of the identifying secret; and

propagating, if the validation result is the successful result, the received user identifier and identifying secret ~~of the user directly~~ from the PSA to one or more target registries ~~if the~~

validation succeeds over third mutually-authenticated secure connections, each of the third connections being between the PSA and a distinct one of the target registries, such that each target registry can store, for the user identifier, a secured version of the identifying secret.

Claims 26 - 27 (canceled)

Claim 28 (currently amended): The method according to Claim 25, wherein the trusted master registry stores password synchronization policy information, and wherein the step of propagating step the received identifying secret further comprises the step of identifying the target registries using the stored password synchronization policy information for the user identifier.

Claim 29 (currently amended): The method according to Claim 25, wherein the trusted master registry stores password synchronization policy information, and wherein the step of propagating step the received identifying secret further comprises the step of identifying the target registries using the stored password synchronization policy information for a user group of which the user identified by the user identifier is a member.

Claims 30 - 32 (canceled)

Claim 33 (currently amended): The method according to Claim 25, wherein the previously-stored secured version of the identifying secret was created, at the trusted master registry, by step of validating further comprises:

performing a security function on a previously-received copy of the ~~received~~ identifying secret of the user, wherein the security function comprises one of (i) a one-way hashing algorithm or (ii) an encryption algorithm;

~~using the received user identifier to locate a previously-stored identifying secret of the user which was stored by the master registry; and~~

wherein the security function is repeated, at the trusted master registry, on the forwarded ~~concluding that the validation succeeds if the located~~ identifying secret of the user, after which, if a result thereof is identical to the previously-stored secured version, the trusted master registry then creates the successful [[a]] result ~~of performing the security function.~~

Claim 34 (currently amended): The method according to Claim 25, wherein the validation result is created, at the trusted master registry, by ~~step of validating further comprises the step of~~ invoking an authenticated LDAP bind or other native authentication mechanism of the trusted master registry, using the forwarded user ~~wherein the received~~ identifier ~~of the user~~ and ~~the~~ ~~received~~ identifying secret of the user, and wherein the validation result is created using a result of the LDAP bind or other native authentication mechanism ~~are passed to the master registry, thereby causing the master registry to validate the passed identifier and identifying secret and return a result which reports a success or failure of the validation.~~

Claim 35 (original): The method according to Claim 25, wherein the PSA has administrative authority for performing operations at the one or more target registries.

Claim 36 (currently amended): The method according to Claim 25, further comprising steps of:

obtaining a new value from the user to be used as the propagated identifying secret if the validation ~~succeeds~~ result is the successful result; and

substituting [[this]] the new value for the received identifying secret prior to operation of the propagating step.

Claim 37 (new): The method according to Claim 25, wherein the forwarding and receiving steps use secure interprocess communications between the PSA and the trusted master registry instead of the second connection.

Claim 38 (new): The method according to Claim 25, wherein the secured version stored by the target registries is not required to be identical to the secured version stored at the trusted master registry.